IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

G.T., by and through next friend LILIANA T. HANLON, SHIMERA JONES, LEROY JACOBS, BALARIE COSBY-STEELE, JOHN DEMATTEO, RICHARD MADAY, MARK HEIL, ALLISON THURMAN, and SHERIE HARRIS, individually, and on behalf of all others similarly situated,

Plaintiffs,

v.

SAMSUNG ELECTRONICS AMERICA, INC. and SAMSUNG ELECTRONICS CO., LTD.,

Defendants.

Civil Action No: 1:21-cv-04976

Hon. Nancy L. Maldonado

SAMSUNG ELECTRONICS AMERICA, INC.'S AND
SAMSUNG ELECTRONICS CO., LTD.'S REPLY IN SUPPORT OF MOTION
TO DISMISS THE CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES

Page(s)

Other Authorities

INTRODUCTION

Plaintiffs' opposition only confirms that the flaws in the CAC are incurable.

Plaintiffs do not dispute that all their BIPA claims require them to establish that Samsung possessed, collected, captured, or otherwise obtained the Face Clustering Data. But they do not point to any factual allegations in the CAC stating that Samsung actually did take any such action with respect to the Face Clustering Data. Instead, their opposition points to allegations that Samsung stores users' ***photographs*** on its servers in the Samsung Cloud and that Samsung controlled the development of the Gallery App ***software*** on Plaintiffs' Galaxy devices. Neither allegation is sufficient to establish BIPA liability. Samsung's actions with respect to the photographs are irrelevant. BIPA expressly does not regulate photographs, and Plaintiffs do not allege that any biometric information or biometric identifiers are stored on cloud servers with the photographs. And Samsung's control over the development of the software used on Plaintiffs' devices does not establish that Samsung had any access to or control over the Face Clustering Data that Plaintiffs contend constitutes biometric data. Were it otherwise, Microsoft would control this reply brief because counsel drafted it using Microsoft Word. Absent any factual allegation that Samsung obtains or has access to the Face Clustering Data, Plaintiffs' conclusory contentions that Samsung possesses, collects, captures, or otherwise obtains supposedly biometric data are flatly inconsistent with the case law interpreting those terms under BIPA, including the very cases that Plaintiffs cite.

Plaintiffs' opposition also does not dispute that the Face Clustering Data does not identify any person and that it is the users, ***not*** Samsung, that supply tags that may identify faces in photographs on the Gallery App. None of Plaintiffs' authorities establish that, under those circumstances, the Face Clustering Data constitutes a biometric identifier or biometric information.

As explained in more detail below and in Samsung's motion to dismiss, the Court should dismiss all of Plaintiffs' claims.

ARGUMENT

I. PLAINTIFFS' BIPA CLAIMS FAIL BECAUSE SAMSUNG DOES NOT "POSSESS" OR "COLLECT" THE FACE CLUSTERING DATA.

Plaintiffs' opposition concedes that to establish liability under BIPA Sections 15(a) and 15(b), they must plead Samsung was "in possession of," "collect[s]," "capture[s]," or "otherwise obtain[s]" biometric data. *See* Opp. at 6, 13; 740 ILCS 14/15(a), (b). They instead argue that Samsung's motion contradicts the CAC's assertion that BIPA was violated. The CAC certainly asserts that violations occurred, but Plaintiffs' opposition does not and cannot point to any factual allegations in the CAC that Samsung possesses or collects, captures, or otherwise obtains the Face Clustering Data. Instead, Plaintiffs point to irrelevant allegations that Samsung stores the photographs, *see* Opp. at 5-6, and that Samsung retains control over the design of the software. Neither allegation is relevant to BIPA liability, as shown below.

A. Plaintiffs Point to No Factual Allegations That Samsung Obtained or Stored Face Clustering Data in the Samsung Cloud.

Contrary to their opposition argument (Opp. § I.A), Plaintiffs do not plausibly allege that Samsung stored—and therefore possessed or obtained—Plaintiffs' biometric data. They point to no factual allegation that the Face Clustering Data ever leaves Plaintiffs' devices because the CAC contains no such allegations. To distract from this failure, Plaintiffs' opposition points to alleged transmission of users' ***photographs*** to Samsung for storage on the Samsung Cloud, hosted on Samsung servers. *See* Opp. at 5-6. This argument mirrors the CAC's allegations that photographs may be stored on the cloud. *See* CAC ¶ 51 ("[T]he Gallery App allows Samsung users to save, organize, edit, share, and store their ***photographs***," citing a Samsung (UK) website explaining that to share photographs across users' devices "[t]he Gallery App can connect to the

Samsung Cloud.") (emphasis added); *id.* ¶ 66 ("Samsung's Gallery App has a feature that allows users to backup [sic] their ***photographs*** to a cloud server.") (emphasis added); *id.* ("Prior to September 2021, those ***photographs*** were uploaded and stored the [sic] Samsung Cloud, a cloud-server created, hosted, and controlled by Samsung.") (emphasis added).

That Samsung allegedly provides a cloud storage service for photographs is completely irrelevant to Plaintiffs' BIPA claims. BIPA expressly excludes photographs from the definition of "biometric identifiers" and "biometric information." *See* 740 ILCS 14/10 ("Biometric identifiers do not include . . . photographs[.]"); *id.* ("Biometric information . . . [must be] based on an individual's biometric identifier."). To state a BIPA claim based on cloud storage, Plaintiffs would have had to allege that data that constitutes biometric information or biometric identifiers are collected in the Samsung Cloud. 740 ILCS 14/15(b). Plaintiffs do not (and cannot) show that their CAC made any such factual allegation about the Face Clustering Data that they alleged to be biometric data under BIPA. *See* Mot. at 6.

Plaintiffs also cannot point to any plausible allegation of Samsung's storage of the Face Clustering Data by referring to the CAC's allegation that the Face Clustering Data is "at least stored locally in centralized databases." Opp. at 5. That argument misstates the CAC, which never alleges storage on a "centralized database" or any Samsung server or database. *See* CAC ¶¶ 51, 66. Further, as explained in Samsung's motion—and as is unrebutted in Plaintiffs' opposition—the CAC's allegation that Face Clustering Data is stored "at least" locally on users' devices, *id.* ¶¶ 5, 54, does not allege any facts about any location other than the user's device where Face Clustering Data is stored. *See* Mot. at 6.

B. **Plaintiffs Do Not Identify Factual Allegations that Samsung's Control Over the Design of the Gallery App Establishes Its Possession and Collection of the Face Clustering Data.**

Plaintiffs' opposition also does not establish that Plaintiffs have adequately alleged facts showing Samsung possessed or obtained the Face Clustering Data on the users' devices. Plaintiffs' opposition instead focuses on allegations in the CAC that Samsung controls the design of the Gallery App software. *See* Opp. at 8-12; CAC ¶¶ 50, 60-65. Plaintiffs argue a defendant's control over allegedly biometric data can be established if the defendant controls the software that dictates how the device collects and stores that data. *See* Opp. at 8-9, 16. But that argument contradicts case law barring BIPA claims against technology manufacturers (like Samsung here) absent specific factual allegations that the manufacturers themselves possessed, collected, or otherwise obtained the data that is alleged to be biometric identifiers or biometric information generated by their products. *Jacobs v. Hanwha Techwin America, Inc.*, 2021 WL 3172967, at *4 (N.D. Ill. Jul. 27, 2021) (dismissing Section 15(a) and 15(b) claims where there was no allegation that the defendant "received" or "could freely access" the data); *Barnett v. Apple, Inc.*, 2022 IL App (1st) 220187 at ¶ 44 (Ill. App. Ct. 1st Dist. Dec. 23, 2022) (dismissing Section 15(a) and 15(b) claims where data was alleged to remain on users' devices and "[t]here is no allegation that Apple stores this information a separate server."). Plaintiffs here do not and cannot allege facts to establish that Samsung has the ability to access, let alone actually collected or came into possession of, the Face Clustering Data on the products it manufactured and sold.

Plaintiffs' contention that Samsung's alleged control over the Gallery App software design (as opposed to control over BIPA-regulated biometric data) is sufficient to state a BIPA claim is unsupported by authority. Plaintiffs argue that the different outcomes in *Hazlitt II* and *Barnett* show that a BIPA claim turns on whether the defendant allegedly has control over the software that collects or generates the user data. *See* Opp. at 10-11 (discussing *Hazlitt v. Apple*

Inc., 543 F. Supp. 3d 643 (S.D. Ill. 2021) ("*Hazlitt II*") and *Barnett*). According to Plaintiffs, the plaintiffs in both *Hazlitt II* and *Barnett* alleged the data was stored on users' devices, and what differentiated the cases was the degree of control Apple exerted over the software. *Id.* On Plaintiffs' reading, the database on the users' devices at issue in *Hazlitt II* was considered Apple's because "the data in it were completely controlled by Apple," but the database on the users' devices at issue in *Barnett* was ***not*** considered Apple's because users could control the software by electing to switch it on or off. *Id.* Plaintiffs argue that their allegations of Samsung's control of the software are "virtually identical" to the allegations deemed sufficient in *Hazlitt II*. *See* Opp. at 7-8.

Yet, Plaintiffs miss the critical distinction between *Hazlitt II* and *Barnett*: the different factual allegations in each of those cases regarding the defendants' ability to access biometrics. Specifically, the *Hazlitt II* court allowed the plaintiffs' complaint to proceed because the plaintiffs had alleged "that ***Apple alone could access the biometric data***." *Hazlitt II*, 543 F. Supp. 3d at 653 (emphasis added). The *Barnett* court, in dismissing BIPA claims, emphasized that the biometric data was stored on the user's device, there was no allegation of any access by Apple, and "[t]here is no allegation that Apple stores this information on a separate server." *Barnett*, 2022 IL App (1st) 220187 at ¶ 44. Here, as in *Barnett* (and unlike in *Hazlitt II*) Plaintiffs make no factual allegation that Samsung has access to the Face Clustering Data stored locally on users' devices. Instead, Plaintiffs rely on allegations about the software Samsung created and put on the device it sold to Plaintiffs: "Samsung, acting through facial recognition software . . . access[es] the biometric data stored in the database" on the users' devices. Opp. at 9. As recognized in *Barnett*, this argument wrongly "equates the product with the company" and cannot survive a motion to dismiss. 2022 IL App (1st) 220187 ¶ 43. Plaintiffs' error is fatal to the Section 15(a) and Section 15(b) claims.

Section 15(a). To Samsung's knowledge, no court has endorsed the view that a device's use of locally stored data establishes the product manufacturer's possession of that data under BIPA Section 15(a). To the contrary, courts permit Section 15(a) claims where plaintiffs make factual allegations that the defendant itself had access to the allegedly biometric data and dismiss Section 15(a) claims absent such allegations. *Compare Barnett*, 2022 IL App (1st) 220187 at ¶ 44 (dismissing Section 15(a) claim where biometric data was allegedly stored on users' devices and "[t]here is no allegation that Apple stores this information a separate server"); *Stauffer v. Innovative Heights Fairview Height, LLC*, No. 19-L-311 at 3 (St. Clair Cnty., Ill., July 23, 2022) (dismissing Section 15(a) claim where the defendant never took "actual direct possession of the data," and ruling that "until [defendant] accesses the information or data in the system [which it had not], [it] does not have possession")[1]; *with Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 282, 284 (N.D. Ill. 2019) (allowing Section 15(a) claim to proceed where the plaintiff's employer had allegedly "disclose[d] . . . fingerprint data" to the defendant)[2]; *Hazlitt v. Apple*, No. 3:20-CV-421-NJR, Dkt. 135 at 11 (S.D. Ill. Aug. 1, 2022) ("*Hazlitt III*") (allowing Section 15(a) claim to proceed where plaintiffs had alleged that Apple "transfers [the] Sync Data . . . [at issue] to Apple's servers via the cloud" and "maintains and stores encryption keys that enable it to access the Sync Data.").[3]

[1] Plaintiffs do not address *Stauffer* in their opposition.

[2] Plaintiffs do not address *Namuwonge* in their opposition.

[3] Plaintiffs' attempt to distinguish *Hazlitt III* on the ground that some limited discovery had occurred beforehand, Opp. at 16 n. 7, is beside the point. *Hazlitt III* is one of many examples establishing the scope of BIPA, regardless of discovery.

The other cases Plaintiffs cite on Section 15(a) likewise confirm that alleging the defendant's access to biometric data (as distinct from its control over the technology) is necessary to state a claim:

- *Mayhall v. Amazon Web Services*, allowed BIPA claims to proceed where the plaintiff alleged that "Defendants obtain the facial scan data . . . and convert the data into face geometry ***on Defendants' servers utilizing Defendants' cloud-computing power.***" 2022 WL 2718091, at *7 (W.D. Wash. May 24, 2022) (emphasis added).
- *Smith v. Signature Systems* allowed BIPA claims to proceed because plaintiffs had alleged that "Signature 'indefinitely stores ***in an electronic database, digital copies of its client's employees' fingerprints . . . in its databases of fingerprints in Illinois***." 2022 WL 595707, at *4 (N.D. Ill. Feb. 28, 2022) (emphasis added).
- *Johnson v. NCR Corp.* allowed BIPA claims to proceed against NCR on allegations that the device at issue "***transmits the acquired biometric data to NCR's servers***," and that NCR "actively manages, maintains, and stores data collected . . . including biometric data, in a ***single, centralized location on its hosted environments and servers***." 2023 WL 1779774, at *1, *4 (N.D. Ill. Feb. 6, 2023) (emphasis added).

In contrast, Plaintiffs here do not point in their opposition to any allegation that the Face Clustering Data is stored on Samsung's servers or that Samsung otherwise had access to the data. Rather, their allegations concede that the Face Clustering Data remains on users' individual devices. *See* CAC ¶¶ 5, 54 (alleging that the Face Clustering Data is stored in the solid-state memory on the user's device).

Section 15(b).

Plaintiffs' pleading similarly fails to support a claim that Samsung violated BIPA Section 15(b) by collecting, capturing, or otherwise obtaining allegedly biometric data. Samsung cannot have collected, captured, or otherwise obtained data that it cannot access in the first place—a logical conclusion only further confirmed by the cases Plaintiffs discuss in opposition.

As noted above and further explained in Samsung's motion, *Barnett* defeats Plaintiffs' claim under Section 15(b) because, like the plaintiffs in *Barnett*, Plaintiffs have failed to allege that Samsung received or had access to the data at issue. *See* Mot. at 7-8. Plaintiffs cannot avoid *Barnett*'s impact on their Section 15(b) claim by erroneously contending that *Barnett* defined "collect" and "capture" differently than the Illinois Supreme Court did in its recent decision in *Cothron v. White Castle System Inc.*, 2023 IL 128004 (Ill. 2023). Opp. at 17. To the contrary, *Cothron* and *Barnett* used functionally identical definitions for "collect" and "capture." *Compare Cothron*, 2023 IL 128004 at ¶ 23 (citing Webster's Third New International Dictionary and defining "collect" as "to receive, gather, or exact ***from a number of persons or other sources***," and defining "capture" as "to take, seize, or catch") (emphasis added); *with Barnett*, 2022 IL App. 220187 ¶ 48-49 (citing the Merriam-Webster Online Dictionary and defining "collect" as "to gather or exact ***from a number of persons or sources***" and "to gather an accumulation of," and defining "capture" as "to record in a permanent file") (emphasis added).)

Cothron's discussion of Section 15(b) confirms that no Section 15(b) claim lies against a defendant that (like Samsung here) has no access to biometric information or biometric identifiers. The court explained that "[t]he active verbs used in Section 15(b)—collect, capture, purchase, receive, and obtain—all mean to gain control." 2023 IL 128004 at ¶ 16. It also ruled that "collect" means "to receive, gather, or exact from a number of persons or other sources" and that to "capture" means "to take, seize, or catch." *Id.* ¶ 23. Samsung did none of these things.

Nor does *Cothron*'s application of the law to facts support Plaintiffs. In *Cothron*, the court expressly "assume[d], without deciding" that White Castle had collected or captured the plaintiff's biometric data because the plaintiff had alleged that "White Castle obtains an employee's fingerprint and stores it in ***its*** database," making the data accessible to White Castle itself and White Castle's third-party storage vendors. *Cothron*, 2023 IL 128004 at ¶ 23 (emphasis added); *see also Cothron v. White Castle System, Inc.*, 477 F. Supp. 3d 723, 727 (N.D. Ill. 2020) ("[a]ccording to [the plaintiff], White Castle's system involved transferring the fingerprints to two third-party vendors . . . as well as storing the fingerprints at other separately owned and operated data-storage facilities"). By contrast, Plaintiffs here concede that the Face Clustering Data is stored only on their own individual devices. *See* CAC ¶¶ 5, 54, 57, 58, 60, 64, 73-74. They do not allege that the Face Clustering Data is stored anywhere beyond their devices, let alone in a server that is accessible to Samsung. And, as explained above, Samsung does not control the Face Clustering Data itself simply because it had control over the design of the software installed on the users' devices.

Heard v. Becton, Dickinson & Co., 524 F. Supp. 3d 831 (N.D. Ill. 2021) ("*Heard II*") further illustrates that a defendant's access to data is a predicate to a Section 15(b) claim. Plaintiffs cite *Heard II* for the proposition that Samsung took an "active step" towards collection by "embed[ding] into all Samsung Devices facial recognition technology." Opp. at 15. But in an earlier decision, the court in *Heard* had dismissed plaintiff's Section 15(b) claim because the plaintiff had failed to allege that the defendant took an "active step" to "bring into [its] possession" his biometric data. *See Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 966

(N.D. Ill. 2020) ("*Heard I*"). The *Heard II* court allowed the plaintiff's amended Section 15(b) claim to proceed precisely because the amended complaint added allegations that the defendant stored his biometric data in ***its own*** servers. *Heard II*, 524 F. Supp. 3d at 841 ("[T]he FAC alleges that . . . the Pyxis system . . . stores users' biometric information both on the device and in BD's servers. Data from subsequent scans are also stored on BD's servers. These allegations suggest that BD itself plays an active role in collecting or otherwise obtaining users' biometric information from Pyxis devices."). No such allegation has been made here.

In addition to *Cothron* and *Heard II,* and the *Mayhall*, *Smith*, and *Johnson* decisions discussed above (*infra* at 7), Plaintiffs' other authorities cited to support their Section 15(b) claims are unavailing and actually support Samsung's position. Each of these cases involved clear factual allegations that the defendant itself had access to the allegedly biometric data.

- *Svoboda v. Amazon.com, Inc.* allowed plaintiffs' Section 15(a) and 15(b) claims to proceed where the complaint "plausibly alleg[ed] that ***the biometrics would go to Amazon's system and Amazon . . . would store the information*** . . ." No. 1:21-cv-05336, Hr'g Tr. at 7:7-11, April 28, 2022, Pl.'s Ex. 1 (emphasis added).
- *Vance v. Amazon, Inc.* and *Vance v. Microsoft Corp.*, allowed BIPA claims to proceed because the defendant had allegedly applied for and downloaded a dataset that contained the plaintiffs' biometric data, which the court reasoned was sufficient to allege the defendant had "obtained" the data and was able to "use[]" it. *Vance,* 525 F. Supp. 3d 1301, 1312-1313 (W.D. Wash. 2021); *Vance*, 525 F. Supp. 3d 1287, 1297-1298 (W.D. Wash. 2021).
- *Rogers v. BNSF*, 2022 WL 787955 (N.D. Ill. Mar. 15, 2022) denied the defendant's motion for summary judgment because "BNSF employees were also involved in the

> registration of drivers," which involved the fingerprint scanning, and received training on how to operate the fingerprint scanners. *Id.* at *7. Examining all evidence favorably towards the plaintiff, the court ruled that a jury could find that the defendant collected, captured, received through trade, or otherwise obtained biometric data because the defendant's employees were actively involved in fingerprint scanning. *Id.* at *7.

The Court should also reject Plaintiffs' attempt to characterize Samsung's control over the relevant software design as the hiring of an "agent" for whose activities Samsung is responsible. Opp. at 19. Samsung's design of the Gallery App does not make the Gallery App an "agent" of Samsung when a user deploys it for the user's own purposes; indeed, software is not a person who can be an "agent" of the designer at all. *See* Restatement (Third) Of Agency § 1.04, Cmt. e (2006) ("[A] computer program is not capable of acting as a principal or agent" because "computer programs are instrumentalities of the person who uses them."); *see also Pekin Life Ins. Co. v. Schmid Family Irrevocable Trust*, 359 Ill. App. 3d 674, 680 (Ill. App. Ct. 1st Dist. 2005) ("An agent is an individual who has a fixed and permanent relation to the companies he represents and who has certain duties and allegiances to such companies.") (internal citation omitted); *Eychaner v. Gross*, 269 Ill. Dec. 80, 99 (Ill. 2002) ("An agent is one who undertakes to manage the affairs of another, on the authority and for the account of the latter, who is called the principal, to render an account to the principal.").

Because Plaintiffs have not sufficiently alleged that Samsung possesses, collects, captures, or otherwise obtains the Face Clustering Data, all of their BIPA claims under both Sections 15(a) and 15(b) must be dismissed.

II. THE FACE CLUSTERING DATA AT ISSUE IS NEITHER A "BIOMETRIC IDENTIFIER" NOR "BIOMETRIC INFORMATION" BECAUSE IT DOES NOT IDENTIFY PARTICULAR INDIVIDUALS.

BIPA regulates only biometric data that identifies specific individuals, *see* 740 ILCS 14/5 (discussing legislative findings and intent of BIPA), but Plaintiffs do not allege that the Face Clustering Data identifies particular individuals, or even could be used to identify particular individuals. The CAC should be dismissed on this independent basis as well.

To mask their inability to plead facts that the Face Clustering Data itself identifies anyone, Plaintiffs make two flawed arguments. First, they argue that they need not allege that "biometric identifiers" identify an individual. *See* Opp. at 20. Second, they argue that the data is a "biometric identifier" and "biometric information" because they have sufficiently alleged that "Samsung creates the Face Clustering Templates for the sole purpose of identifying the person" because "Samsung uses [them] to recognize [a] person" and group photographs likely to contain similar individuals "underneath a circular frame showing the face of the 'identified individual.'" Opp. at 21 (citing CAC ¶¶ 5, 55-56). Plaintiffs are wrong on both points.

First, Plaintiffs' assertion that they need not allege that the supposed "biometric identifiers" actually identify an individual ignores the text of BIPA itself. As the legislature made very clear, BIPA only regulates data that is "biologically ***unique to [an] individual.***" 740 ILCS 14/5(c). Thus, BIPA regulates only data that ***identifies*** particular individuals. Plaintiffs' assertion that they need not allege the Face Clustering Data can be used to identify particular individuals to fall within the definition of "biometric identifier," Opp. at 20-21, is plainly inconsistent with the text and legislative intent of BIPA. *See generally Lacey v. Vill. Of Palatine*, 904 N.E.2d 18, 25 (Ill. 2009) (holding that a court must give effect to the legislature's intent as evidenced by the plain language of a statute).

Second, Plaintiffs' assertion that the Face Clustering Data identifies particular individuals because Samsung "uses [the Face Clustering Data] to recognize" individuals highlights Plaintiffs' fundamental misunderstanding of what it means to "identify." The allegations in the CAC merely establish that the Gallery App can "recognize" that a face in an analyzed photograph is similar to a face in an already-stored photograph, such that the two photographs can be grouped together. But even under the CAC allegations, it is the user (if they so choose)—***not*** Samsung—that supplies the actual identity of the individual in the photograph. Indeed, Plaintiffs' authorities contradict their assertion that they need not allege that "biometric identifiers" identify individuals. In each case that Plaintiffs rely on for the proposition that it is sufficient to allege, without more, that data is a "biometric identifier," the data at issue was alleged to ***actually identify*** individuals.

- In *Carpenter v. McDonald's Corp.,* the plaintiffs alleged that an "AI voice assistant extracts the customer's voiceprint biometrics to determine . . . ***identifying information such as the customer's age, gender, accent, nationality, and national origin*** . . . [and] utilize[s] voiceprint recognition in combination with license plate scanning technology to ***identify unique customers . . .***" Complaint, No. 1:21-cv-02906, Dkt. 1-1 at ¶¶ 20-21 (N.D. Ill.) (emphasis added). The court allowed the plaintiff's Section 15(b) claim to proceed because "importantly, Plaintiff alleges that McDonald's uses the AI and data to ***actually identify unique individuals.***" *Carpenter v. McDonald's Corp.*, 580 F. Supp. 3d 512, 517 (N.D. Ill. 2022) (emphasis added). The court confirmed the claim would fail if discovery disproved the allegation and showed the data at issue did not uniquely identify specific individuals. *Id.* at 517-518. The *Carpenter* footnote Plaintiffs cite adds nothing because it merely explains that a plaintiff need not allege that they—personally—were "identified as speaking[.]" *Id.* at 518 n. 2.

- In *Goree v. New Albertsons, L.P., d/b/a Jewel Osco,* the plaintiffs alleged that they were "required to repeatedly read long lists of certain words into the system that allows the Vocollect software to create a template of the voice of that particular worker and trains the voice recognition software to understand and ***identify the voice of that particular worker.***" Complaint, No. 22-cv-01738, Dkt. 1-2 ¶¶ 35-36 (N.D. Ill.) (emphasis added). The crux of the court's decision on the motion to dismiss was "the allegations in the complaint that the voiceprints at issue ***could be used to identify individuals***." *Goree*, 1:22-cv-01738 (N.D. Ill.), Hr'g Tr. at 16:22-25, Mar. 8, 2022, Pl.'s Ex. 2.
- In *Hazlitt v. Apple*, the plaintiff alleged that "***[n]ot only does Defendant use face geometries to identify individuals***, with iOS version 11 it uses face geometries to model users faces and track the user's expressions in real time . . . After biometric identifiers are collected and Defendant's software has a sufficient sampling of images, ***the Photos App applies an algorithm to identify the Apple Device user . . .***" Complaint, No. 3:20-cv-00421, Dkt. 1-1 ¶¶ 72, 101 (S.D. Ill.). The court focused on the fact that the plaintiffs "allege[d] that the Photos app applies an algorithm to identify the device user." *Hazlitt v. Apple*, 500 F. Supp. 3d 738, 749 (S.D. Ill. 2020) *("Hazlitt I")*.
- In *Rivera v. Google*, the plaintiffs alleged that "[t]hese unique face templates are not only collected and used by Google Photos to ***identify individuals by name, but also to recognize their gender, age, and location.***" Amended Complaints, No. 1:16-cv-

> 02714, Dkts. 40, 41 ¶ 23 (N.D. Ill.). The defendant moved to dismiss, but the court allowed the BIPA claims to proceed because "Google is creating a set of biology-based measurements ('biometric') ***that is used to identify a person ('identifier').***" *Rivera v. Google*, 238 F. Supp. 3d 1088, 1095 (N.D. Ill. 2017).

Unlike the data at issue in *Carpenter*, *Goree*, *Hazlitt*, and *Rivera*, the Face Clustering Data is not alleged to identify particular individuals (nor do Plaintiffs argue as much in their opposition).

Nor have Plaintiffs sufficiently alleged that the Face Clustering Data identifies particular individuals. In each of *In re Facebook Biometric Privacy Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016); *Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103 (N.D. Ill. 2015); *Monroy v. Shutterfly, Inc.*, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017); and *Rivera*, 238 F.Supp.3d at 1088, the technology at issue allegedly involved databases of biometric data that the defendant then used to supply the name of individuals who appeared in photographs. In its opening brief, Samsung explained that the key allegation was that the defendant in those cases supplied the identity. *See* Mot. at 13-15. Here, by contrast, only the user of the Samsung device can supply the identity (*not* Samsung)—a key distinction that Plaintiffs did not address in their opposition. *E.g.*, CAC ¶ 180 ("Plaintiff Maday . . . has 'tagged' individuals in photographs that Samsung has organized by facial geometry.").

Plaintiffs' opposition does not address the fundamental point that the CAC does not allege that the Face Clustering Data itself identifies anyone. Plaintiffs allege only that the Gallery App can organize and sort photos by comparing the Face Clustering Data in newly stored photos against the Face Clustering Data in already-stored photos, CAC ¶¶ 5, 55-56, 88-90, 101-10, and that *users* can supply tags to images with matching Face Clustering Data. *Id.* ¶ 52. Plaintiffs are thus wrong in arguing that they alleged facts to establish that the device identified the individuals. *See* Opp. at 21. Grouping similar faces (done by the Gallery App on the device) is not identification of the faces (done by the user of the device). *See* Definition of *Identify*, merriam-webster.com, https://www.merriam-webster.com/dictionary/identify ("identify" means "to perceive or state the identity of (someone or something)," or "to ascertain the identity of (someone or something that is unfamiliar or unknown)").

III. <u>CONCLUSION</u>

Because Plaintiffs have failed to allege facts sufficient to state a claim that Samsung violated BIPA, the Court should dismiss Plaintiffs' CAC with prejudice.

Dated: April 17, 2023

By: /s/ *Randall W. Edwards*
Randall W. Edwards

ATTORNEY FOR DEFENDANTS
SAMSUNG ELECTRONICS AMERICA, INC. and
SAMSUNG ELECTRONICS CO., LTD.

DONOHUE BROWN MATHEWSON & SMYTH LLC
Mark H. Boyle
140 South Dearborn Street, Suite 800
Chicago, IL 60603
(312) 422-0900

O'MELVENY & MYERS LLP
Randall W. Edwards
Matthew D. Powers (*pro hac vice*)
Two Embarcadero Center, 28th Floor
San Francisco, CA 94111-3823
(415) 984-8700

Ashley M. Pavel
610 Newport Center Dr., 17th Floor
Newport Beach, CA 92660
(949) 823-6900

Attorneys for Defendants
Samsung Electronics America, Inc. and
Samsung Electronics Co., Ltd.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on the 17th of April, 2023, he caused the foregoing DEFENDANTS SAMSUNG ELECTRONICS AMERICA, INC.'S AND SAMSUNG ELECTRONICS CO., LTD.'S REPLY IN SUPPORT OF MOTION TO DISMISS THE CONSOLIDATED AMENDED CLASS ACTION COMPLAINT to be filed with the Clerk of the District Court via the CM/ECF system, which will send notification of such filing to all counsel of record at the email addresses on file with the Court.

By: /s/ *Randall W. Edwards*
Randall W. Edwards

ATTORNEY FOR DEFENDANTS
SAMSUNG ELECTRONICS AMERICA, INC.
and SAMSUNG ELECTRONICS CO., LTD.

O'MELVENY & MYERS LLP
Randall W. Edwards
Two Embarcadero Center, 28th Floor
San Francisco, CA 94111-3823
(415) 984-8700